Quantum Computation:
Zusammenfassung der 13. Vorlesung (13.02.09)

2.3,2 *Auswertung durch Kettenbruchentwicklung (Fortsetzung)*

Wir hatten [12. Vorlesung, p.4]für $2 \leq n \leq N$ schon gefolgert, dass

$$x = [a_o a_1 a_2 \dots a_N] = \frac{a'_n p_{n-1} + p_{n-2}}{a'_n q_{n-1} + q_{n-2}},$$

oder für $1 \leq n \leq N-1$

$$x = [a_o a_1 a_2 \dots a_N] = \frac{a'_{n+1} p_n + p_{n-1}}{a'_{n+1} q_n + q_{n-1}}$$

ist. Für die Differenz von x und dem n-ten Näherungsbruch ergibt sich deshalb

$$\begin{aligned} x - \frac{p_n}{q_n} &= \frac{q_n(a'_{n+1}p_n + p_{n-1}) - p_n(a'_{n+1}q_n + q_{n-1})}{q_n(a'_n q_{n-1} + q_{n-2})} \\ &= \frac{q_n p_{n-1} - p_n q_{n-1}}{q_n(a'_{n+1}q_n + q_{n-1})} = \frac{(-1)^n}{q_n(a'_{n+1}q_n + q_{n-1})}. \end{aligned}$$

Überdies gilt noch

$$x = a_0 + \frac{1}{a'_1} \quad \text{so dass} \quad x - \frac{p_0}{q_0} = x - a_0 = \frac{1}{a'_1} = \frac{(-1)^0}{a'_1}.$$

Mit den Definitionen

$$q'_1 := a'_1, \quad q'_n := a'_n q_{n-1} + qn - 2 \ \ (2 \leq n \leq N-1), \quad q'_n := q_n$$

ergibt sich der

Satz: Für $1 \leq n \leq N-1$ ist

$$x - \frac{p_n}{q_n} = \frac{(-1)^n}{q_n q'_n}$$

Nun ist $0 < a_2 \in \mathbf{N}$, und damit

$$q_1 = a_1 < a_1' < a_1 + 1 = q_1 + q_0 \leq a_2 q_1 + q_0 = q_2.$$

Mit Ausnahme des Falles $a_{N-1}' = a_{n-1} + 1$, wenn $a_N = 1$ ist, gilt

$$a_{n+1} < a_{n+1}' = a_{n+1} + \frac{1}{[a_{n+2} a_{n+3} \dots a_N]} < a_{n+1} + 1,$$

so dass

$$q_{n+1} = a_{n+1} q_n + q_{n-1} < a_{n+1}' q_n + q_{n-1} < q_{n+1}',$$

und weiter

$$q_{n+1}' = a_{n+1}' q_n + q_{n-1} < (a_{n+1}+1) q_n + q_{n-1} = q_{n+1} + q_n \leq a_{n+2} q_{n+1} + q_n = q_{n+2}.$$

Nun gilt

$$x - \frac{p_n}{q_n} = \frac{(-1)^n}{q_n q_n'} \quad \text{bzw.} \quad \frac{1}{q_{n+1}'} = (-1)^n (q_n x - p_n),$$

und damit für $1 \leq n \leq N-2$

$$\frac{1}{q_{n+2}} < \frac{1}{q_{n+1}'} = |q_n x - p_n| < \frac{1}{q_{n+1}}$$

Für $n = N-1$ bzw. $n = N$ gilt

$$|q_{N-1} x - p_{N-1}| < \frac{1}{q_N} \quad \text{und} \quad |q_N x - p_N| = 0,$$

und im Ausnahmefall, wenn $a_{N-1}' = a_{N-1} + 1$ und $a_N = 1$ ist, folgt

$$q_{N-1}' = (a_{N-1} + 1) q_{N-2} + q_{N-3} = q_{N-1} + q_{N-2} =_N q_{N-1} + q_{N-2} = q_N.$$

Im Ausnahmefall gilt daher nach dem letzten Satz

$$\frac{1}{q_{N-1}'} = |q_{N-1} x - p_{N-1}| = \frac{1}{q_N}.$$

Wegen $q_{N-1} < q_{N-2}$ können wir die Ergebnisse der vorstehenden Rechnung im folgenden Satz zusammenfassen.

Satz: Für einfachz Kettenbrüche endlicher Läng $N > 1$ gelten für $1 \leq n \leq N$

$$|q_n x - p_n| > |q_{n+1} x - p_{n+1}| \quad \text{bzw.} \quad |x - \frac{p_n}{q_n}| > |x - \frac{p_{n+1}}{q_{n+1}}|$$

und für $1 \leq n \leq N-1$

$$q_n x - p_n = \frac{(-1)^n \delta_n}{q_{n+1}} \quad \text{wobei} \quad 0 < \delta_n \begin{cases} < 1 & \text{für} \quad 1 \leq n \leq N-2 \\ = 1 & \text{für} \quad n = N-1 \end{cases}$$

und

$$\left| x - \frac{p_n}{q_n} \right| < \frac{1}{q_n q_{n+1}} < \frac{1}{q_n^2} \quad \text{für} \quad 1 \leq n \leq N-2,$$

$$\left.\begin{array}{ll} |x - \frac{p_{N-1}}{q_{N-1}}| < \frac{1}{q_{N-1} q_N} < \frac{1}{q_N^2} & \text{im Normalfall,} \\ |x - \frac{p_{N-1}}{q_{N-1}}| = \frac{1}{q_{N-1}} & \text{im Ausnahmefall} \end{array}\right\} \quad \text{für } n = N-1.$$

Die folgenden Sätze führen zu dem erstaunlichen Ergehnis, dass ein Quotient ganzer Zahlen ein Näherungbruch sein muss, wenn er nur nahe genug am Wert $x$des Kettenbruches liegt. Dieses Ergebnis ist deshalb so erstaunlich, weil die rationalen Zahlen auf der reellen Achse überall dicht liegen, aber eine offene Umgebung von x ausgezeichet werden kann, in der alle Brüche mit gegebenem Nenner Näherungsbrüche sind.

Satz: Sei $x \in \mathbf{Q}$ und

$$x = \frac{P\zeta + R}{Q\zeta + S},$$

wobei $0 < \zeta \in \mathbf{R}$, $P, Q, R, S \in \mathbf{Z}$, $Q > S > 0$ und $PS - QR = \pm 1$, dann sind $\frac{R}{S}$ und $\frac{P}{Q}$ aufeinander folgende Näherungsbrüche von einer Kettenbruchdarstellung von x. Gilt $\frac{R}{S} = \frac{p_{n-1}}{q_{n-1}}$ und $\frac{P}{Q} = \frac{p_n}{q_n}$, dann ist ζ der $(n+1)$-te vollständige Nenner.

Beweis: Da $\frac{P}{Q} = [a_0 a_1 a_2 \ldots a_n]$ mit geradem und ungeradem n möglich ist, kann o.B.d.A. angenommen werden, dass $PS - QR = (-1)^{n-1}$ ist. Da $S, R \in \mathbf{Z}$ ist, enthält der von P und Q erzeugt Modul ganzer Zahlen die 1 und damit gilt $(P, Q) = 1$. Ferner ist nach Voraussetzng $Q > 0$. Weil mit

$\frac{P}{Q} = [a_0 a_1 a_2 \dots a_n]$ anderersits $\frac{P}{Q} = \frac{p_n}{q_n}$, $((p_n, q_n) = 1$ und $q_n > 0$ gilt, ist $PP = p_n$ und $Q = q_M$. Daraus folgt

$$p_n S - q_n n R = PS - QR = (-1)^{M-1} = p_n q_{n-1} - p_{n-1} q_n$$

und somit

$$p_n(S - q_{n-1}) = q_n(R - p_{n-1}).$$

Weeil nun

$$q_n | p_n(S - q_{n-1}), \qquad p_n | q_n(R - p_{n-1}), \qquad (p_n, q_n) = 1$$

gelten, folgen

$$q_n | (S - q_{n-1}), \qquad p_n | (R - p_{n-1}).$$

Aderersets folgt aus $Q = q_n > S > 0$ und $q_n > q_{n-1} > 0$ sowohl $q_n > S - q_{n-1}$ als auch $q_n > q_{n-1} - S$, also $q_n > |S - q_{n-1}|$. Dies widersprich aber $q_n | p_n(S - q_{n-1})$, wenn nicht $S = q_{n-1}$ ist. Aus $S = q_{n-1}$ folgt aber auch $R = p_{n-1}$. Damit ist die erste Behautung des atzzes gezeigt. Nach der Voraussetzung ist nun

$$x = \frac{p_n \zeta + p_{n-1}}{q_n \zeta + q_{n-1}}$$

und $x \in \mathbf{Q}$. Dann ist auch $\zeta \in \mathbf{Q}$ und nach Voraussetzung ist $\zeta > 0$, so dass mit $\zeta = [a_{n+1} a_{n+2} \dots a_N]$ gilt

$$x = [a_0 a_1 a_2 \dots a_n \zeta] = [a_0 a_1 a_2 \dots a_n a_{n+1} a_{n+2} \dots a_N].$$

Der nächste Satz zeigt, dass in der Umgebung $(x - \frac{p_n}{q_n}, x - \frac{p_n}{q_n})$ keine Quotienten $\frac{P}{Q}$ mit $(P, Q) = 1$ und $0 < Q \leq q_n$ enthalten sind.

Satz: Sei $x \in \mathbf{Q}$ und $1 \leq n \leq N - 2$. Wenn $P, Q \in \mathbf{N}$, $0 < Q \leq q_n$ und $\frac{P}{Q} \neq \frac{p_n}{q_n}$, dann gilt

$$|q_n x - p_n| < |Qx - P|.$$

Beweis: O.B.d.A. sei $(P, Q) = 1$. Da stets

$$q_n x - p_n| < |q_{n-1} x - p_{n-1}|$$

gilt, genügt es, den Fall $q_{n-1} < Q \leq q_n$ zu betrachten. - Im Fall $Q = q_n$ ist $P \neq p_n$ und damit

$$\left|\frac{p_n}{q_n} - \frac{P}{q_n}\right| \geq \frac{1}{q_n}.$$

Andererseits ist wegen $q_{n+1} \geq n+1$

$$\left|x - \frac{p_n}{q_n}\right| < \frac{1}{q_n q_{n+1}} \leq \frac{1}{(n+1)q_n} < \frac{1}{2q_n},$$

so dass

$$\left|x - \frac{p_n}{q_n}\right| < \frac{1}{2}\left|\frac{p_n}{q_n} - \frac{P}{q_n}\right| \leq \frac{1}{2}\left(\left|x - \frac{p_n}{q_n}\right| + \left|x - \frac{P}{q_n}\right|\right)$$

und wegen $Q = q_n$

$$\frac{1}{2}\left|x - \frac{p_n}{q_n}\right| < \frac{1}{2}\left|x - \frac{P}{q_n}\right| \quad \Longrightarrow \quad |q_n x - p_n| < |Qx - P|.$$

- Im Fall $q_{n-1} < Q < q_n$ kann wegen $(P.Q) = 1$ weder $\frac{P}{Q} = \frac{p_{n-1}}{q_{n-1}}$ noch $\frac{P}{Q} = \frac{p_{n-1}}{q_n}$. denn jede derGleichungen würde der Teilerfremdheit von P und Q widersprechen. Das Gleichungsystem

$$\mu p_n + \nu p_{n-1} = P, \qquad \mu q_n + \nu q_{n-1} = Q$$

hat eine ganzzahlige Lösung, denn

$$\begin{aligned} Pq_{n-1} - Qp_{n-1} &= (\mu p_n + \nu p_{n-1})q_{n-1} - (\mu q_n + \nu q_{n-1})p_{n-1} \\ &= \mu(p_n q_{n-1} - p_{n-1}q_n) = \mu(-1)^{n+1}, \end{aligned}$$

also

$$\mu = (-1)^{n+1}(Pq_{n-1} - Qp_{n-1});$$

und

$$\begin{aligned} Pq_n - Qp_n &= (\mu p_n + \nu p_{n-1})q_n - (\mu q_n + \nu q_{n-1})p_n \\ &= \nu(p_{n-1}q_n - q_{n-1}p_n) = \nu(-1)^n, \end{aligned}$$

also

$$\nu = (-1)^n(Pq_n - Qp_n).$$

Ferner ist

$$\begin{aligned} Qx - P &= (\mu q_n + \nu q_{n-1})x - (\mu p_n + \nu p_{n-1}) \\ &= \mu(q_n x - p_n) + \nu(q_{n-1}x - p_{n-1}) \end{aligned}$$

und weil $\operatorname{sgn}(q_n x - p_n) = (-1)^n$ ist, sind beide Terme auf der rechten Seite negativ. Es gilt deshalb

$$\begin{aligned} |Qx - P| &= |\mu(q_n x - p_n)| + |\nu(q_{n-1}x - p_{n-1})| \\ &> |\mu||q_n x - p_n| > |q_n x - p_n|, \end{aligned}$$

denn $|\mu| \in \mathbf{N}$.

Satz: Von zwei aufeinander folgenden Näherungsbrüchen erfüllt wenigstens einer, $\frac{p}{q} \in \{\frac{p_n}{q_n}, \frac{p_{n+1}}{q_{n+1}}\}$, $1 \leq n \leq N-2$, die Ungleichung

$$\left| x - \frac{p}{q} \right| < \frac{1}{2q^2}.$$

Beweis: O.B.d.A. nehmen wir an, dass

$$\frac{p_n}{q_n} < x < \frac{p_{n+1}}{q_{n+1}},$$

dann ist

$$\left| \frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n} \right| = \left| \frac{p_{n+1}}{q_{n+1}} - x \right| + \left| x - \frac{p_n}{q_n} \right|.$$

Die Annahme

$$\left| x - \frac{p_n}{q_n} \right| \geq \frac{1}{2q_n^2} \qquad \text{und} \qquad \left| x - \frac{p_{n+1}}{q_{n+1}} \right| \geq \frac{1}{2q_{n+1}^2}$$

führt auf

$$\frac{1}{q_n q_{n+1}} = \left| \frac{p_{n+1 q_n} - p_n q_{n+1}}{q_n q_{n+1}} \right| = \left| \frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n} \right| \geq \frac{1}{2q_n^2} + \frac{1}{2q_{n+1}^2},$$

und daraus folgt

$$0 \geq \frac{(q_{n+1 q_n})^2}{2q_n^2 q_{n+1}^2}$$

im Widerspruch zu $q_n < q_{n+1}$.

Wir formulieren nun den für die Auswertung des Quantenalgorithmus zur Ordnungsbestimmung entscheidenden Satz. Es sei bemerkt, dass dieser Satz auch für $x \in \mathbf{R}$ bewiesen werden kann, wenn man Kettenbrüche unendlicher Länge betrachtet.

Satz: Sei $x \in \mathbf{Q}$ und $p, q \in \mathbf{N}$. Gilt

$$\left| x - \frac{p}{q} \right| < \frac{1}{2q^2},$$

dann ist $\frac{p}{q}$ ein Näherungsbruch von x.

Beweis: Für $x \neq \frac{p}{q}$ ist nachVoraussetzung

$$x - \frac{p}{q} = \frac{\epsilon\Theta}{q^2}, \quad \epsilon = \pm 1, \quad 0 < \Theta < \frac{1}{2}.$$

Ferner sei $\frac{p}{q} = [a_o a_1 a_2 \dots a_n]$, wobei o.B.d.A. $\epsilon = (-1)^n$ gelte und $\frac{p}{q} = \frac{p_n}{q_n}$ ist. Durch

$$x = \frac{\omega p_n + p_{n-1}}{\omega q_n + q_{n-1}}$$

liegt $\omega \in \mathbf{Q}$ fest und es ist

$$\begin{aligned} \frac{\epsilon\Theta}{q^2} &= \frac{\omega p_n + p_{n-1}}{\omega q_n + q_{n-1}} - \frac{p_n}{q_n} = \frac{q_n(\omega p_n + p_{n-1}) - p_n(\omega q_n + q_{n-1})}{q_n(\omega q_n + q_{n-1})} \\ &= \frac{q_n p_{n-1} - p_n q_{n-1}}{q_n(\omega q_n + q_{n-1})} = \frac{(-1)^n}{q_n(\omega q_n + q_{n-1})} = \frac{\epsilon}{q_n(\omega q_n + q_{n-1})}. \end{aligned}$$

Daraus folgt

$$\omega = \frac{1}{\Theta} - \frac{q_{n-1}}{q_n} > 2 - 1 = 1.$$

Mit $\mathbf{Q} \ni \omega = [a_{n+1} a_{n+2} \dots a_N]$ ist somit $x = [a_o a_1 a_2 \dots a_n a_{n+1} a_{n+2} \dots a_N]$ und $\frac{p}{q} = \frac{p_n}{q_n}$ ist n-ter Näherungsbruch.

Dieser Satz sagt aus, dass $\frac{s}{r}$ ein Näherungsbruch des Messwertes κ nach einem Lauf des Quantenalgorithmus zur Ordnungbestimmung ist, wenn nur

$$\left| \kappa - \frac{s}{r} \right| < \frac{1}{2r^2},$$

erfüllt ist. Ein Messwert

$$\kappa \in \mathcal{M}_r := \bigcup_{s=0}^{r-1} [\frac{s}{r} - \epsilon, \frac{s}{r} + \epsilon]$$

erfüllt diese Voraaussetzung sicher, wenn $\epsilon < \frac{1}{2M^2}$ und $\kappa > \epsilon$ ist, denn es ist zum einen $r < M$ und zum anderen kann $\frac{s}{r} = 0$ kein Näherungsbruch sein kann. Wenn $\kappa \in \mathcal{M}_r$ ist, müssen die ersten $K = \log(2M^2)$ Dualstellen hinter dem Komma richtig sein. Dies tritt allerdings nur mit einer Wahrscheinlichkeit

$$q_{|d|\leq\epsilon}(\delta) \geq \frac{1 - \cos(2^{N+1}\pi\delta)}{8} \left(\frac{1}{2^N\delta(1 - 2^N\delta)} - \frac{2}{(2^{N-K-1} + 1)} \right)$$

ein. In dem günstigen Fall $2^N\delta = \frac{1}{2}$ ist

$$q_{|d|\leq\epsilon}(\delta) \geq 1 - \frac{1}{2(2^{N-K-1} + 1)}.$$

In jedem Fall sollte $N > K = \log(2M^2) + 1$ gewält werden und diesen Wert hinreichend weit übertreffen, um diese Wahrschinlichkei zu optimieren. Für $2^N\delta = \frac{1}{2}$ ist bei Wahl von $N = \log(2M^2) + 7$ diese Wahrscheinlichkeit schon größer als $1 - \frac{1}{100}$. Da die Werte $s = 0, 1, 2, \ldots, (r-1)$ gleichverteilt sind, ist für $\frac{s}{r} > 0$ die Wahrscheichkeit $\frac{r-1}{r}$. Die Auswertung endet damit, im Fall $\kappa > \epsilon$ unter Verwendung klassischer Rechner die Ornung unter den Nennern der Näherungsbrüche und deren Vielfachen zu suchen. Im Falle $\kappa < \epsilon$ oder vergeblicher Suche ist der Vorgang zu wiederholen. Mit Wahrscheinlichkeit $\frac{r-1}{r}(1 - \frac{1}{100})$ wird im günstigen Fall $2^N\delta = \frac{1}{2}$ die Ordnung in einem einzigen Lauf des Algorithmus bestimmt.